

SUM-PRODUCT PHENOMENA: p -ADIC CASE.

ALIREZA SALEHI GOLSEFIDY

ABSTRACT. The sum-product phenomena over a finite extension K of \mathbb{Q}_p is explored. The main feature of the results is the fact that they only depend on the ramification index of K .

1. INTRODUCTION

1.1. Main results. One of the main results of this note is the uniform version of [BG09, Proposition 3.3].

Theorem 1. *For any $0 < \varepsilon \ll 1$ and positive integer e , there are $0 < \delta := \delta(\varepsilon, e)$, and positive integer $C := C(\varepsilon, e)$, such that for any finite extension K of \mathbb{Q}_p with large, depending on ε and e , residue field \mathfrak{f} and ramification index at most e the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Suppose $A \subseteq \mathcal{O}$ such that

$$|\pi_{\mathfrak{p}^N}(A)| \geq |\mathfrak{f}|^{N\varepsilon}.$$

Then

$$\pi_{\mathfrak{p}^{N_2}}(\mathfrak{p}^{N_1} \mathbb{Z}x) \subseteq \pi_{\mathfrak{p}^{N_2}}(\langle A \rangle_C),$$

for some $x \in \mathcal{O}^\times$ and integers N_1 and N_2 such that

$$N\delta + N_1 \leq N_2 \leq NC,$$

where $\langle A \rangle_j := \sum_j \prod_j A - \sum_j \prod_j A$, $\sum_j A := \{\sum_{i=1}^j a_i \mid a_i \in A\}$, and $\prod_j A := \{\prod_{i=1}^j a_i \mid a_i \in A\}$.

The inductive argument in proof of [BG09, Proposition 3.1] implies that the following is a corollary of Theorem 1.

Corollary 2. *For any $0 < \varepsilon \ll 1$ and positive integers e, d_0 , there are $0 < \delta := \delta(\varepsilon, e, d_0)$, and positive integer $C := C(\varepsilon, e, d_0)$, such that for any finite extension K of \mathbb{Q}_p with large, depending on ε and e , residue field \mathfrak{f} and ramification index at most e the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Suppose $A \subseteq \mathcal{O}^{d_0} := \mathcal{O} \times \cdots \times \mathcal{O}$ such that

$$|\pi_{\mathfrak{p}^N}(A)| \geq |\mathfrak{f}|^{N\varepsilon}.$$

Then

$$\pi_{\mathfrak{p}^{N_2}}(\mathfrak{p}^{N_1} \mathbb{Z}\mathbf{x}) \subseteq \pi_{\mathfrak{p}^{N_2}}(\langle A \rangle_C),$$

for some $\mathbf{x} \in \mathcal{O}^{d_0} \setminus \mathfrak{p}\mathcal{O}^{d_0}$, and integers N_1 and N_2 such that

$$N\delta + N_1 \leq N_2 \leq NC.$$

The other important corollary of Theorem 1 is its global version, which generalizes [Bor08, Corollary, Part I.1] from \mathbb{Q}_p to any finite extension K of \mathbb{Q}_p .

Date: February 2, 2016.

1991 *Mathematics Subject Classification.* 11B75.

A. S-G. was partially supported by the NSF grant DMS-1303121, the A. P. Sloan Research Fellowship. Parts of this work was done when I was visiting Isaac Newton Institute and the MSRI, and I would like to thank both of these institutes for their hospitality.

Corollary 3. *For any $0 < \varepsilon \ll 1$ and positive integers d and d_0 , there are $0 < \delta := \delta(\varepsilon, d, d_0)$, and positive integer $C := C(\varepsilon, d, d_0)$, such that for any finite extension k of \mathbb{Q} of degree at most d the following holds:*

Let \mathcal{O}_k be the ring of integers of k , and \mathfrak{p} be a non-zero prime ideal of \mathcal{O}_k . Suppose $A \subseteq \mathcal{O}_k^{d_0} := \mathcal{O}_k \times \cdots \times \mathcal{O}_k$ such that

$$|\pi_{\mathfrak{p}^N}(A)| \geq |\mathcal{O}_k/\mathfrak{p}|^{N\varepsilon}.$$

Then

$$\pi_{\mathfrak{p}^{N_2}}(\{i\mathbf{x} \mid i \in \mathbb{Z} \cap \mathfrak{p}^{N_1}\}) \subseteq \pi_{\mathfrak{p}^{N_2}}(\langle A \rangle_C),$$

for some $\mathbf{x} \in \mathcal{O}_k^{d_0} \setminus \mathfrak{p}^d \mathcal{O}_k^{d_0}$, and integers N_1 and N_2 such that

$$N\delta + N_1 \leq N_2 \leq NC.$$

Proof. For any \mathfrak{p} , the ramification index of the completion $K := k_{\mathfrak{p}}$ of k with respect to the \mathfrak{p} -adic topology is at most d . Let $\mathcal{O}_{\mathfrak{p}}$ be the ring of integers of K , and $\tilde{\mathfrak{p}}$ be a uniformizing element of $\mathcal{O}_{\mathfrak{p}}$. Then it is well-known that $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \langle \tilde{\mathfrak{p}} \rangle$ and the embedding of \mathcal{O}_k into $\mathcal{O}_{\mathfrak{p}}$ induces isomorphism between $\pi_{\mathfrak{p}^N}(\mathcal{O}_k)$ and $\pi_{\tilde{\mathfrak{p}}^N}(\mathcal{O}_{\mathfrak{p}})$.

Now if $|N_{k/\mathbb{Q}}(\mathfrak{p})| \gg_{\varepsilon, d, d_0} 1$, we get the desired result by Corollary 2. For the finitely many remaining primes, we get the desired result by [BG09, Proposition 3.3]. \square

Remark 4. *Corollary 3 is an important ingredient of getting the \mathfrak{p} -adic super approximation, see [SG-a, SG-b].*

To prove Theorem 1, we start by showing a scalar-sum-product expansion result:

Theorem 5 (Scalar-Sum-Product expansion). *For any $\varepsilon > 0$, $0 < \delta \ll \varepsilon^5$, and any finite extension K of \mathbb{Q}_p with large, depending on ε , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Let $\Omega \subseteq \mathcal{O}$, and suppose $\pi_{\mathfrak{p}}$ induces a bijection between $\Omega \subseteq \mathcal{O}$ and \mathfrak{f}^{\times} . Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that

- (1) $|A| \leq |\mathfrak{f}|^{N(1-\varepsilon)}$,
- (2) $|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon}$ for any $N\delta \leq i \leq N$.
- (3) *there are $a_{01}, a_{02}, a_{11}, a_{12} \in A$ such that $a_{i1} - a_{i2} \in \pi_{\mathfrak{p}^N}(\mathfrak{p}^i \mathcal{O} \setminus \mathfrak{p}^{i+1} \mathcal{O})$.*

Then

$$\max_{\omega \in \Omega} |\langle A \rangle_6 + \pi_{\mathfrak{p}^N}(\omega) \langle A \rangle_6| \geq |A| |\mathfrak{f}|^{N\delta}.$$

Similar to all the previous works on expansion (either under two operations or one), there is an underline bounded generation result. Typically one uses the expansion result to enlarge the set to certain extent and then use Fourier analysis, e.g. Sarnak-Xue trick, quasi-randomness, exponential sum estimates, to finish the process in finitely many steps. The same strategy is used to prove Proposition 26. Based on Proposition 26 and a propagation process, we get the following refiner result (which is needed in the proof of Theorem 1).

Theorem 6. *For any $0 < \varepsilon_1 \ll \varepsilon_2 \ll 1$, a positive integer m , $0 < \delta \ll_{m, \varepsilon_1} 1$, positive integers $1 \ll_{m, \varepsilon_1} C$ (number of needed sum-product) and $1 \ll_{\varepsilon_1} k$ (number of needed scalars) and any finite extension K of \mathbb{Q}_p with large, depending on ε_1 , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Let $\Omega \subseteq \mathcal{O}$, and suppose $\pi_{\mathfrak{p}}$ induces a bijection between $\Omega \subseteq \mathcal{O}$ and \mathfrak{f}^{\times} . Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that

- (1) $|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon_1}$ for any $N\delta \leq i \leq N$.
- (2) *there are $a_{01}, a_{02}, a_{11}, a_{12} \in A$ such that $a_{i1} - a_{i2} \in \pi_{\mathfrak{p}^N}(\mathfrak{p}^i \mathcal{O} \setminus \mathfrak{p}^{i+1} \mathcal{O})$.*

Then

$$\pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon_2^m N \rceil} \mathcal{O}) \subseteq \langle A \rangle_C + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_C + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \langle A \rangle_C,$$

for some $\omega_i \in \prod_k (\Omega \cup \{1\})$.

As a corollary of Theorem 6, we immediately get the uniform version of [BG09, Corollary A.1].

Corollary 7. *For any $0 < \varepsilon_1 \ll \varepsilon_2 \ll 1$, $0 < \delta \ll_{\varepsilon_1} 1$, and positive integer $1 \ll_{\varepsilon_1} C$, and any finite extension K of \mathbb{Q}_p with large, depending on ε_1 , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that

- (1) $|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon_1}$ for any $N\delta \leq i \leq N$.
- (2) $\pi_{\mathfrak{p}^{e'}}(A) = \pi_{\mathfrak{p}^{e'}}(\mathcal{O})$, where $e' = 1$ if K is an unramified extension, and $e' = 2$ otherwise.

Then

$$\pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon_2 N \rceil} \mathcal{O}) \subseteq \sum_{C_1} \prod_{C_2} A - \sum_{C_1} \prod_{C_2} A,$$

for some integers $C_1, C_2 \leq C$.

Proof. Since $\pi_{\mathfrak{p}^{e'}}(A) = \pi_{\mathfrak{p}^{e'}}(\mathcal{O})$, we have $\pi_{\mathfrak{p}}(A) = \mathfrak{f}$. Therefore there is a subset $\Omega \subseteq A$ such that $\pi_{\mathfrak{p}}$ induces a bijection between Ω and \mathfrak{f}^\times . If K is ramified over \mathbb{Q}_p , then $e' = 2$. So by the assumption, we can apply Theorem 6 to $\Omega \subseteq A$ and A , which implies the claim. Now suppose K is an unramified extension of \mathbb{Q}_p , and let $s : \mathfrak{f} \rightarrow \pi_{\mathfrak{p}^2}(A)$ be a section of $\pi_{\mathfrak{p}} : \pi_{\mathfrak{p}^2}(A) \rightarrow \mathfrak{f}$. Since K is an unramified extension of \mathbb{Q}_p , \mathfrak{f} cannot be embedded into $\pi_{\mathfrak{p}^2}(\mathcal{O})$ as an additive group. Hence there are $x_1, x_2 \in \mathfrak{f}$ such that $s(x_1) + s(x_2) - s(x_1 + x_2) \neq 0$. Therefore this time we can apply Theorem 6 to $\Omega \subseteq A$ and $\langle A \rangle_2$ and get the claim. \square

1.2. Application. My main motivation to get such uniform sum-product results was to prove a *uniform p -adic super approximation* [SG-a, SG-b], which has many applications, e.g. orbit equivalence rigidity, Banach-Ruziewicz problem, variations of ℓ -adic Galois representations, etc.

1.3. Notation. In this note, K is a finite extension of \mathbb{Q}_p , \mathcal{O} is its ring of integers, $\mathfrak{p}|p$ is a uniformizing element, $\mathfrak{f} := \mathcal{O}/\langle \mathfrak{p} \rangle$ is its residue field, and e is the ramification index of K over \mathbb{Q}_p , i.e. $\langle p \rangle = \langle \mathfrak{p}^e \rangle$. For any non-negative integer m , $\pi_{\mathfrak{p}^m} : \mathcal{O} \rightarrow \mathcal{O}/\langle \mathfrak{p}^m \rangle$ is the residue map.

We use the usual Vinogradov notation: $x \gg y$ means that there is a universal positive constant c such that $x \geq cy$, and $x \gg_{z_1, z_2} y$ means that there is a positive function $c(z_1, z_2)$ of z such that $x \geq c(z_1, z_2)y$.

ACKNOWLEDGEMENTS

I am in debt of P. Varjú for explaining to me his joint work in progress with E. Lindenstrauss, where they give a new proof of a sum-product result for $\mathbb{Z}/2^N\mathbb{Z}$. I would like to thank E. Lindenstrauss for the fruitful conversations that helped me to strengthen my initial results. I would like to again thank E. Lindenstrauss and P. Varjú for allowing me to include slight variation of some their arguments before the completion of their work. Finally I would like to thank J. Bourgain for our enlightening communications regarding this problem.

2. SCALAR-SUM-PRODUCT PHENOMENA.

In this section, using Lindenstrauss-Varjú's [LV] method we study *sum-product-scalar product properties* of ring of integers \mathcal{O} of an unramified extension K of \mathbb{Q}_p .

2.1. Scalar-Sum inequality for regular sets. The main goal of this section is to prove Proposition 8.

Proposition 8 (Scalar-Sum inequality for regular sets). *Let K be a finite extension of \mathbb{Q}_p , \mathcal{O} be its ring of integers, and \mathfrak{f} be its residue field. Let $\Omega \subseteq \mathcal{O}$ be such that $\pi_{\mathfrak{p}}$ induces a bijection between Ω and $\mathfrak{f}_{\mathfrak{p}}^\times$.*

Let A and B be (m_0, \dots, m_{N-1}) -regular and (l_0, \dots, l_{N-1}) -regular¹. subsets of $\pi_{\mathbf{p}^N}(\mathcal{O})$, respectively. Then

$$\max_{\omega \in \Omega} |A + \pi_{\mathbf{p}^N}(\omega)B| \geq \prod_{i=0}^{N-1} \max \left(1, \left(\frac{1}{m_i l_i} + \frac{1}{|\mathbf{f}|} \right)^{-1} \right).$$

Let us fix a subset $\Omega \subseteq \mathcal{O}^\times$ such that $\pi_{\mathbf{p}}$ induces a bijection between Ω and \mathbf{f}^\times . Let $\psi : \mathbf{f} \rightarrow \Omega \cup \{0\}$ be such that $\pi_{\mathbf{p}}(\psi(\alpha)) = \alpha$ for any $\alpha \in \mathbf{f}$. We can treat $\Omega \cup \{0\}$ as a set of \mathbf{p} -adic digits: for any $x \in \mathcal{O}$ we get a unique sequence $\{D_n(x)\}_{n=0}^\infty$ of elements of \mathbf{f} such that

$$(1) \quad x = \sum_{n=0}^{\infty} \psi(D_n(x)) \mathbf{p}^n.$$

Having the D_n 's, we get a family of sections ψ_n of $\pi_{\mathbf{p}^n}$, i.e.

$$(1) \quad \psi_n : \pi_{\mathbf{p}^n}(\mathcal{O}) \rightarrow \mathcal{O}, \quad \psi_n(\pi_{\mathbf{p}^n}(x)) := \sum_{i=0}^{n-1} \psi(D_i(x)) \mathbf{p}^i.$$

$$(2) \quad \pi_{\mathbf{p}^n} \circ \psi_n = \text{id}_{\pi_{\mathbf{p}^n}(\mathcal{O})}.$$

For any $n < N$, we have that $\psi_{n,N} := \pi_{\mathbf{p}^N} \circ \psi_n$ is a section of $\pi_{\mathbf{p}^n} : \pi_{\mathbf{p}^N}(\mathcal{O}) \rightarrow \pi_{\mathbf{p}^n}(\mathcal{O})$. In particular, $\psi_{0,n} = \pi_{\mathbf{p}^n} \circ \psi$.

One can visualize \mathcal{O} as an infinite rooted $|\mathbf{f}|$ -regular tree. We can use the digits to label children of any vertex. I.e. for any $\bar{x} = \mathbf{p}^n \mathcal{O} + x \in \pi_{\mathbf{p}^n}(\mathcal{O})$ let

$$\theta_{\bar{x}} : \mathbf{f} \rightarrow \pi_{\mathbf{p}^{n+1}}(\mathbf{p}^n \mathcal{O} + x), \quad \theta_{\bar{x}}(\alpha) := \pi_{\mathbf{p}^{n+1}}(\psi_n(\bar{x}) + \psi(\alpha) \mathbf{p}^n).$$

Having a probability measure μ on $\pi_{\mathbf{p}^N}(\mathcal{O})$, for any $\bar{x} := \mathbf{p}^n \mathcal{O} + x \in \pi_{\mathbf{p}^n}(\mathcal{O})$, one gets a conditional measure on $\pi_{\mathbf{p}^{n+1}}(\mathbf{p}^n \mathcal{O} + x)$ if $\mu(\pi_{\mathbf{p}^n}(x)) \neq 0$ ². The pull back of this conditional measure via $\theta_{\bar{x}}$ gives us a probability measure on \mathbf{f} and it is denoted by $\mu_{\bar{x}}$. And so for any $\alpha \in \mathbf{f}$ we have

$$(2) \quad \mu_{\bar{x}}(\alpha) = \frac{\pi_{\mathbf{p}^{n+1}}[\mu](\theta_{\bar{x}}(\alpha))}{\pi_{\mathbf{p}^n}[\mu](\bar{x})}.$$

Definition 9. A subset A of $\pi_{\mathbf{p}^N}(\mathcal{O})$ is called an $(m_0, m_1, \dots, m_{N-1})$ -regular subset if for any $0 \leq n \leq N-1$ and $\bar{x} := \mathbf{p}^n \mathcal{O} + x$ we have that either $\bar{x} \notin \pi_{\mathbf{p}^n}(A)$ or

$$|\pi_{\mathbf{p}^{n+1}}(A) \cap \pi_{\mathbf{p}^{n+1}}(\mathbf{p}^n \mathcal{O} + x)| = m_n.$$

Lemma 10. Let A be an (m_0, \dots, m_{N-1}) -regular subset of $\pi_{\mathbf{p}^N}(\mathcal{O})$. Let \mathcal{P}_A be the probability counting measure on A . Then, for any $\bar{x} := x + \mathbf{p}^k \mathcal{O}$, we have that $\pi_{\mathbf{p}^k}[\mathcal{P}_A] = \mathcal{P}_{\pi_{\mathbf{p}^k}(A)}$, and $(\mathcal{P}_A)_{\bar{x}}$ is a probability counting measure on a subset of order m_k of \mathbf{f} .

Proof. Both of the above claims are easy consequences of the fact that A is a regular set. □

For any $\alpha \in \mathbf{f}$ and a non-negative integer k , there is a map $\sigma_{\alpha,k} : \pi_{\mathbf{p}^k}(\mathcal{O}) \times \pi_{\mathbf{p}^k}(\mathcal{O}) \rightarrow \mathbf{f}$ such that for any $\bar{x}_1, \bar{x}_2 \in \pi_{\mathbf{p}^k}(\mathcal{O})$ we have

$$(3) \quad \psi_k(\bar{x}_1 + \psi_{0,k}(\alpha) \bar{x}_2) - \psi_k(\bar{x}_1) - \psi(\alpha) \psi_k(\bar{x}_2) + \psi(\sigma_{\alpha,k}(\bar{x}_1, \bar{x}_2)) \mathbf{p}^k \in \mathbf{p}^{k+1} \mathcal{O}.$$

Lemma 11. Let A and B be (m_0, \dots, m_{N-1}) -regular and (l_0, \dots, l_{N-1}) -regular subsets of $\pi_{\mathbf{p}^N}(\mathcal{O})$, respectively. Then for any $\bar{x} \in \pi_{\mathbf{p}^k}(\mathcal{O})$ and $\alpha \in \mathbf{f}$ we have

$$(\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B)_{\bar{x}} = \sum_{\bar{x}_1 + \psi_{0,k}(\alpha) \bar{x}_2 = \bar{x}} \frac{\pi_{\mathbf{p}^k}[\mathcal{P}_A](\bar{x}_1) \pi_{\mathbf{p}^k}[\mathcal{P}_B](\bar{x}_2)}{\pi_{\mathbf{p}^k}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\bar{x})} \lambda_{\sigma_{\alpha,k}(\bar{x}_1, \bar{x}_2)}((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2}),$$

where $\lambda_{\beta}(\mu)(\bullet) := \mu(\bullet - \beta)$ and $\sigma_{\alpha,k}$ is defined as in (3).

¹For the definition of a regular set, see Definition 9.

²In this article, since we are working with probability measures on finite sets, we identify a measure with its distribution function.

Proof. By the definition of $(\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B)_{\bar{x}}$ (see (2)), one needs to compute $\pi_{\mathfrak{p}^{k+1}}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\theta_{\bar{x}}(\beta))$ for $\beta \in \mathfrak{f}$. We have

$$\pi_{\mathfrak{p}^{k+1}}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\theta_{\bar{x}}(\beta)) = \sum \mathcal{P}_A(x_1) \mathcal{P}_B(x_2)$$

where the sum is over $x_1, x_2 \in \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that $\pi_{\mathfrak{p}^{k+1}}(x_1 + \psi_{0,N}(\alpha)x_2) = \psi_{k,k+1}(\bar{x}) + \psi_{0,k+1}(\beta)\pi_{\mathfrak{p}^{k+1}}(\mathfrak{p}^k)$. These conditions just depend on $\pi_{\mathfrak{p}^{k+1}}(x_i)$. Hence by regularity of A and B and Lemma 10 we have that

$$\pi_{\mathfrak{p}^{k+1}}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\theta_{\bar{x}}(\beta)) = \sum \mathcal{P}_{\pi_{\mathfrak{p}^{k+1}}(A)}(x'_1) \mathcal{P}_{\pi_{\mathfrak{p}^{k+1}}(B)}(x'_2)$$

where the sum is over $x'_1, x'_2 \in \pi_{\mathfrak{p}^{k+1}}(\mathcal{O})$ such that $x'_1 + \psi_{0,k+1}(\alpha)x'_2 = \psi_{k,k+1}(\bar{x}) + \psi_{0,k+1}(\beta)\pi_{\mathfrak{p}^{k+1}}(\mathfrak{p}^k)$. Now first we fix $\bar{x}_i = \pi_{\mathfrak{p}^k}(x'_i)$ and then parametrize possible x'_i by elements of \mathfrak{f} using $\theta_{\bar{x}_i}$. Hence we have

$$\pi_{\mathfrak{p}^{k+1}}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\theta_{\bar{x}}(\beta)) = \sum_I \sum_{II} \mathcal{P}_{\pi_{\mathfrak{p}^{k+1}}(A)}(\theta_{\bar{x}_1}(\alpha_1)) \mathcal{P}_{\pi_{\mathfrak{p}^{k+1}}(B)}(\theta_{\bar{x}_2}(\alpha_2))$$

where the first sum is over $\bar{x}_1, \bar{x}_2 \in \pi_{\mathfrak{p}^k}(\mathcal{O})$ such that $\bar{x}_1 + \psi_{0,k}(\alpha)\bar{x}_2 = \bar{x}$, and the second sum is over $\alpha_1, \alpha_2 \in \mathfrak{f}$ such that

$$(4) \quad \theta_{\bar{x}_1}(\alpha_1) + \psi_{0,k+1}(\alpha)\theta_{\bar{x}_2}(\alpha_2) = \psi_{k,k+1}(\bar{x}) + \psi_{0,k+1}(\beta)\pi_{\mathfrak{p}^{k+1}}(\mathfrak{p}^k).$$

By the definition of $\theta_{\bar{x}_i}$, we have that (4) holds if and only if

$$(5) \quad (\psi_{0,k+1}(\alpha_1) + \psi_{0,k+1}(\alpha)\psi_{0,k+1}(\alpha_2) - \psi_{0,k+1}(\beta))\pi_{\mathfrak{p}^{k+1}}(\mathfrak{p}^k) = \psi_{k,k+1}(\bar{x}) - \psi_{k,k+1}(\bar{x}_1) - \psi_{0,k+1}(\alpha)\psi_{k,k+1}(\bar{x}_2).$$

And by the definition (see (3)) of $\sigma_{\alpha,k}$ we have that (5) holds if and only if

$$(6) \quad \alpha_1 + \alpha\alpha_2 = \beta + \sigma_{\alpha,k}(\bar{x}_1, \bar{x}_2).$$

Therefore we have

$$\pi_{\mathfrak{p}^{k+1}}[\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B](\theta_{\bar{x}}(\beta)) = \sum \pi_{\mathfrak{p}^k}[\mathcal{P}_A](\bar{x}_1) \pi_{\mathfrak{p}^k}[\mathcal{P}_B](\bar{x}_2) \lambda_{\sigma_{\bar{x},k}(\bar{x}_1, \bar{x}_2)}((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2})$$

where the sum is over $\bar{x}_1, \bar{x}_2 \in \pi_{\mathfrak{p}^k}(\mathcal{O})$ such that $\bar{x}_1 + \psi_{0,k}(\alpha)\bar{x}_2 = \bar{x}$. So by (2) we are done. \square

Before stating a corollary of Lemma 11, let us recall the definition and basic properties of entropy of a probability measure.

Definition 12. Let X be a finite set and μ be a probability measure on X .

(1) The (Shannon) entropy $H(\mu)$ of μ is

$$H(\mu) := \sum_{x \in X} -\mu(x) \log \mu(x).$$

(2) Suppose \mathcal{B} is a partition of X . Then the entropy of \mathcal{B} with respect to μ is

$$H(\mu; \mathcal{B}) := \sum_{A \in \mathcal{B}} -\mu(A) \log \mu(A).$$

(3) Suppose $\mathcal{B}_1, \mathcal{B}_2$ are two partitions of X . Suppose \mathcal{B}_2 is refiner than \mathcal{B}_1 (it is denoted by $\mathcal{B}_1 \preceq \mathcal{B}_2$), i.e. for any $A_2 \in \mathcal{B}_2$ there is $A_1 \in \mathcal{B}_1$ such that $A_2 \subseteq A_1$. Then the conditional entropy $H(\mu; \mathcal{B}_2 | \mathcal{B}_1)$ is defined as follows

$$H(\mu; \mathcal{B}_2 | \mathcal{B}_1) := \sum_{A \in \mathcal{B}_1} \mu(A) \sum_{A' \in \mathcal{B}_2, A' \subseteq A} -\frac{\mu(A')}{\mu(A)} \log \frac{\mu(A')}{\mu(A)}.$$

Lemma 13. Suppose X is a finite set, and μ is a probability measure on X . Then

(1) For any partitions $\mathcal{B}_1 \preceq \mathcal{B}_2$ of X , we have $H(\mu; \mathcal{B}_2) = H(\mu; \mathcal{B}_1) + H(\mu; \mathcal{B}_2 | \mathcal{B}_1)$. In particular for any partition \mathcal{B} we have $H(\mu) = H(\mu; \mathcal{B}) + H(\mu; \{\{x\} | x \in X\} | \mathcal{B})$.

- (2) The entropy function is concave on the space of probability measures, i.e. for any probability measures μ_i on X and numbers $a_i \in [0, 1]$ that add up to one we have

$$H\left(\sum_{i=1}^n a_i \mu_i\right) \geq \sum_{i=1}^n a_i H(\mu_i).$$

- (3) We have $H(\mu) \leq \log |\text{supp } \mu|$.

- (4) We have $H(\mu) \geq -\log \|\mu\|_2^2$, where $\|\mu\|_2^2 := \sum_{x \in X} \mu(x)^2$.

Proof. All of the above properties (maybe except the last one) are well-known. So I will prove only the last property. Since $f(x) = -\log x$ is a concave function, we have

$$f(\|\mu\|_2^2) = f\left(\sum_{x \in X} \mu(x)\mu(x)\right) \leq \sum_{x \in X} \mu(x)f(\mu(x)).$$

□

Corollary 14. Let A and B be (m_0, \dots, m_{N-1}) -regular and (l_0, \dots, l_{N-1}) -regular subsets of $\pi_{\mathbf{p}^N}(\mathcal{O})$, respectively. Then for any $\alpha \in \mathfrak{f}^\times$ we have

$$H(\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B; \mathcal{B}_{k+1} | \mathcal{B}_k) \geq \frac{1}{|\pi_{\mathbf{p}^k}(A)| |\pi_{\mathbf{p}^k}(B)|} \sum_{\bar{x}_1 \in \pi_{\mathbf{p}^k}(A), \bar{x}_2 \in \pi_{\mathbf{p}^k}(B)} H((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2}),$$

where \mathcal{B}_i is the partition of $\pi_{\mathbf{p}^N}(\mathcal{O})$ that comes from $\pi_{\mathbf{p}^i}$.

Proof. By the definition of conditional entropy we have

$$(7) \quad H(\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B; \mathcal{B}_{k+1} | \mathcal{B}_k) = \sum_{\bar{x} \in \pi_{\mathbf{p}^k}(\mathcal{O})} \pi_{\mathbf{p}^k}[\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B](\bar{x}) H((\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B)_{\bar{x}}).$$

Now we notice that

$$\sum_{\bar{x}_1 + \psi_{0,k}(\alpha)\bar{x}_2 = \bar{x}} \pi_{\mathbf{p}^k}[\mathcal{P}_A](\bar{x}_1) \pi_{\mathbf{p}^k}[\mathcal{P}_B](\bar{x}_2) = \pi_{\mathbf{p}^k}[\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B](\bar{x})$$

as B is a regular set. Hence by Lemma 11 and the concavity of entropy we have

$$(8) \quad H((\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B)_{\bar{x}}) \geq \sum_{\bar{x}_1 + \psi_{0,k}(\alpha)\bar{x}_2 = \bar{x}} \frac{\pi_{\mathbf{p}^k}[\mathcal{P}_A](\bar{x}_1) \pi_{\mathbf{p}^k}[\mathcal{P}_B](\bar{x}_2)}{\pi_{\mathbf{p}^k}[\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B](\bar{x})} H(\lambda_{\sigma_{\alpha,k}(\bar{x}_1, \bar{x}_2)}((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2}))$$

Therefore by (7), (8), and $H(\lambda_{\sigma_{\alpha,k}(\bar{x}_1, \bar{x}_2)}((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2})) = H((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2})$ we have

$$\begin{aligned} H(\mathcal{P}_A * \psi_{0,N}(\alpha)\mathcal{P}_B; \mathcal{B}_{k+1} | \mathcal{B}_k) &\geq \sum_{\bar{x} \in \pi_{\mathbf{p}^k}(\mathcal{O})} \sum_{\bar{x}_1 + \psi_{0,k}(\alpha)\bar{x}_2 = \bar{x}} \pi_{\mathbf{p}^k}[\mathcal{P}_A](\bar{x}_1) \pi_{\mathbf{p}^k}[\mathcal{P}_B](\bar{x}_2) H((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2}) \\ &\geq \frac{1}{|\pi_{\mathbf{p}^k}(A)| |\pi_{\mathbf{p}^k}(B)|} \sum_{\bar{x}_1 \in \pi_{\mathbf{p}^k}(A), \bar{x}_2 \in \pi_{\mathbf{p}^k}(B)} H((\mathcal{P}_A)_{\bar{x}_1} * \alpha(\mathcal{P}_B)_{\bar{x}_2}) \end{aligned}$$

by regularity of A and B . □

Lemma 15. Let \bar{A}, \bar{B} be two non-empty subsets of a finite field \mathfrak{f} . Then

$$\frac{1}{|\mathfrak{f}^\times|} \sum_{\alpha \in \mathfrak{f}^\times} \|\mathcal{P}_{\bar{A}} * \alpha \mathcal{P}_{\bar{B}}\|_2^2 \leq \min \left(1, \frac{1}{|\bar{A}| |\bar{B}|} + \frac{1}{|\mathfrak{f}|} \right).$$

Proof. Let us recall that for any two subsets X and Y of \mathfrak{f} , the additive energy of X and Y is

$$E(X, Y) = |\{(x_1, y_1, x_2, y_2) \in X \times Y \times X \times Y \mid x_1 + y_1 = x_2 + y_2\}|,$$

and we have

$$E(X, Y) = \|\mathbf{1}_X * \mathbf{1}_Y\|_2^2.$$

where $\mathbf{1}_X$ is the characteristic function of the set X . We have

$$\begin{aligned}
\frac{1}{|\mathfrak{f}^\times|} \sum_{\alpha \in \mathfrak{f}^\times} \|\mathcal{P}_{\overline{A}} * \alpha \mathcal{P}_{\overline{B}}\|_2^2 &= \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} \|\mathbf{1}_{\overline{A}} * \mathbf{1}_{\alpha \overline{B}}\|_2^2 \\
&= \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} E(\overline{A}, \alpha \overline{B}) \\
&= \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} |\{(a_1, b_1, a_2, b_2) \in \overline{A} \times \overline{B} \times \overline{A} \times \overline{B} \mid a_1 + \alpha b_1 = a_2 + \alpha b_2\}| \\
&= \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} \{ (a_1, b_1, a_2, b_2) \in \overline{A} \times \overline{B} \times \overline{A} \times \overline{B} \mid a_1 = a_2, a_1 + \alpha b_1 = a_2 + \alpha b_2 \} \\
&+ \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} \{ (a_1, b_1, a_2, b_2) \in \overline{A} \times \overline{B} \times \overline{A} \times \overline{B} \mid a_1 \neq a_2, a_1 + \alpha b_1 = a_2 + \alpha b_2 \} \\
&= \frac{1}{|\overline{A}| |\overline{B}|} \\
&+ \frac{1}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2} \sum_{\alpha \in \mathfrak{f}^\times} \{ (a_1, b_1, a_2, b_2) \in \overline{A} \times \overline{B} \times \overline{A} \times \overline{B} \mid a_1 \neq a_2, b_1 \neq b_2, \alpha = \frac{a_1 - a_2}{b_2 - b_1} \} \\
&= \frac{1}{|\overline{A}| |\overline{B}|} + \frac{|(\overline{A}^2 \setminus \Delta(\overline{A})) \times (\overline{B}^2 \setminus \Delta(\overline{B}))|}{|\mathfrak{f}^\times| |\overline{A}|^2 |\overline{B}|^2}, \text{ where } \Delta(X) := \{(x, x) \mid x \in X\}, \\
&= \frac{1}{|\overline{A}| |\overline{B}|} + \frac{(|\overline{A}| - 1)(|\overline{B}| - 1)}{|\mathfrak{f}^\times| |\overline{A}| |\overline{B}|} \leq \min \left(1, \frac{1}{|\overline{A}| |\overline{B}|} + \frac{1}{|\mathfrak{f}|} \right).
\end{aligned}$$

□

Proof of Proposition 8. Let us denote the average of a function $f : \mathfrak{f}^\times \rightarrow \mathbb{R}$ by $\mathbb{E}_\alpha f(\alpha)$. We have

$$\begin{aligned}
\max_{\alpha \in \mathfrak{f}^\times} \log |A + \psi_{0,N}(\alpha)B| &\geq \mathbb{E}_\alpha \log |A + \psi_{0,N}(\alpha)B| \\
(\text{by Lemma 13, part 3}) &\geq \mathbb{E}_\alpha H(\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B) \\
(\text{by Lemma 13, part 1}) &\geq \sum_{k=0}^{N-1} \mathbb{E}_\alpha H(\mathcal{P}_A * \psi_{0,N}(\alpha) \mathcal{P}_B; \mathcal{B}_{k+1} | \mathcal{B}_k) \\
(\text{by Corollary 14}) &\geq \sum_{k=0}^{N-1} \frac{1}{|\pi_{\mathfrak{p}^k}(A)| |\pi_{\mathfrak{p}^k}(B)|} \sum_{x_1 \in \pi_{\mathfrak{p}^k}(A), x_2 \in \pi_{\mathfrak{p}^k}(B)} \mathbb{E}_\alpha H((\mathcal{P}_A)_{x_1} * \alpha (\mathcal{P}_B)_{x_2}) \\
(\text{by Lemma 13, part 4}) &\geq \sum_{k=0}^{N-1} \frac{1}{|\pi_{\mathfrak{p}^k}(A)| |\pi_{\mathfrak{p}^k}(B)|} \sum_{x_1 \in \pi_{\mathfrak{p}^k}(A), x_2 \in \pi_{\mathfrak{p}^k}(B)} \mathbb{E}_\alpha \left(-\log \|(\mathcal{P}_A)_{x_1} * \alpha (\mathcal{P}_B)_{x_2}\|_2^2 \right) \\
(\text{by the concavity of } -\log) &\geq \sum_{k=0}^{N-1} \frac{1}{|\pi_{\mathfrak{p}^k}(A)| |\pi_{\mathfrak{p}^k}(B)|} \sum_{x_1 \in \pi_{\mathfrak{p}^k}(A), x_2 \in \pi_{\mathfrak{p}^k}(B)} -\log \mathbb{E}_\alpha \left(\|(\mathcal{P}_A)_{x_1} * \alpha (\mathcal{P}_B)_{x_2}\|_2^2 \right) \\
(\text{by Lemma 15}) &\geq \sum_{k=0}^{N-1} \frac{1}{|\pi_{\mathfrak{p}^k}(A)| |\pi_{\mathfrak{p}^k}(B)|} \sum_{x_1 \in \pi_{\mathfrak{p}^k}(A), x_2 \in \pi_{\mathfrak{p}^k}(B)} \log \left(\max \left(1, \left(\frac{1}{m_k l_k} + \frac{1}{|\mathfrak{f}|} \right)^{-1} \right) \right) \\
&= \sum_{k=0}^{N-1} \log \left(\max \left(1, \left(\frac{1}{m_k l_k} + \frac{1}{|\mathfrak{f}|} \right)^{-1} \right) \right).
\end{aligned}$$

□

2.2. Scalar-Sum-Product expansion for regular sets. The following is the main result of this section.

Proposition 16 (Scalar-Sum-Product expansion for regular sets). *For any $\varepsilon > 0$, $0 < \delta \ll \varepsilon^4$, and any finite extension K of \mathbb{Q}_p with large, depending on ε , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Let $\Omega \subseteq \mathcal{O}$, and suppose $\pi_{\mathfrak{p}}$ induces a bijection between $\Omega \subseteq \mathcal{O}$ and \mathfrak{f}^\times . Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that

- (1) *A is a (m_0, \dots, m_{N-1}) -regular subset, and $m_0, m_1 > 1$.*
- (2) *$|A| \leq |\mathfrak{f}|^{N(1-\varepsilon)}$.*
- (3) *$|\pi_{\mathfrak{p}^l}(A)| \geq |\mathfrak{f}|^{l\varepsilon}$ for any $N\delta \leq l \leq N$.*

Then

$$\max_{\omega \in \Omega, a \in A-A} |A + \pi_{\mathfrak{p}^N}(\omega)aA| \geq |A||\mathfrak{f}|^{N\delta}.$$

We prove Proposition 16 by contradiction. For the rest of this section, A and m_i 's satisfy all the conditions of Proposition 16. And $\psi_{0,N}$'s are defined as in the paragraph of (1). Moreover we assume to the contrary that $|A + \psi_{0,N}(\alpha)aA| < |A||\mathfrak{f}|^{N\delta}$ (for a small enough δ to be determined later) for any $\alpha \in \mathfrak{f}$ and $a \in A - A$, and let

$$(9) \quad x_i := \frac{\log m_i}{\log |\mathfrak{f}|}$$

for any $0 \leq i \leq N-1$.

Lemma 17. *Let x_i 's be as in (9). Then*

$$(10) \quad x_0, x_1 \neq 0, \text{ and } 0 \leq x_i \leq 1, \text{ for any } 0 \leq i \leq N-1,$$

$$(11) \quad \sum_{i=0}^{N-1} x_i \leq N(1-\varepsilon),$$

$$(12) \quad \sum_{i=0}^{l-1} x_i \geq l\varepsilon, \text{ for any } N\delta \leq l \leq N,$$

$$(13) \quad \sum_{i=0}^{N-1-k} \min(x_i, 1 - x_{i+k}) \leq N \left(\delta + \frac{\log 2}{\log |\mathfrak{f}|} \right) \text{ if } x_k \neq 0.$$

Proof. Since $1 \leq m_i \leq |\mathfrak{f}|$, $|A| = \prod_{i=0}^{N-1} m_i \leq |\mathfrak{f}|^{N(1-\varepsilon)}$, and $|\pi_{\mathfrak{p}^l}(A)| = \prod_{i=0}^{l-1} m_i \geq |\mathfrak{f}|^{l\varepsilon}$ for $N\delta \leq l \leq N$, one can see that (10), (11), and (12) hold.

Suppose $x_k \neq 0$. So there is $a \in A - A$ such that $a \in \pi_{\mathfrak{p}^N}(\mathfrak{p}^k \mathcal{O}) \setminus \pi_{\mathfrak{p}^N}(\mathfrak{p}^{k+1} \mathcal{O})$. Hence aA is an $(1, \dots, 1, m_0, \dots, m_{N-1-k})$ -regular subset of $\pi_{\mathfrak{p}^N}(\mathcal{O})$. Let $m_{-i} = 1$ for any $i \in \mathbb{Z}^+$. Therefore by Proposition 8 we have

$$\begin{aligned} \max_{\alpha \in \mathfrak{f}^\times} |A + \psi_{0,N}(\alpha)aA| &\geq \prod_{i=0}^{N-1} \max \left(1, \left(\frac{1}{m_i m_{i-k}} + \frac{1}{|\mathfrak{f}|} \right)^{-1} \right) \\ &\geq \left(\prod_{i=0}^{N-1} m_i \right) \prod_{i=0}^{N-1} \left(\frac{1}{m_{i-k}} + \frac{m_i}{|\mathfrak{f}|} \right)^{-1} \\ &\geq |A| \prod_{i=0}^{N-1} \frac{\min(m_{i-k}, |\mathfrak{f}|/m_i)}{2}. \end{aligned}$$

Thus by the contrary assumption we have

$$N\delta \log |\mathbf{f}| \geq -N \log 2 + \sum_{i=0}^{N-1} \min(\log m_{i-k}, \log |\mathbf{f}| - \log m_i).$$

And so

$$N \left(\delta + \frac{\log 2}{\log |\mathbf{f}|} \right) \geq \sum_{i=0}^{N-1-k} \min(x_i, 1 - x_{i+k}).$$

□

Now we follow Lindenstrauss-Varjú's treatment [LV], almost verbatim, to prove that if $|\mathbf{f}| \gg_\varepsilon 1$ and $0 < \delta \ll \varepsilon^4$, then there are no real numbers x_0, \dots, x_{N-1} that satisfy properties mentioned in Lemma 17. This is based on Mann's theorem on Schnirelmann density of subsets of non-negative integers.

Definition 18. *The Schnirelmann density $\sigma(X)$ of a non-empty subset X of non-negative integers is*

$$\sigma(X) := \inf_{n \in \mathbb{Z}^+} \frac{|X \cap [1, n]|}{n}.$$

Theorem 19 (Mann's Theorem). *Let X, Y be two non-empty subsets of non-negative integers. Suppose X and Y contain 0. Then either $X + Y = \mathbb{Z}^{\geq 0}$ or $\sigma(X + Y) \geq \sigma(X) + \sigma(Y)$.*

For $\{x_k\}$ as in Equation(9), let

$$(14) \quad B := \{k \in [0, N-1] \mid x_k \neq 0\}.$$

Lemma 20 (Lindenstrauss-Varjú [LV]). *Let x_i 's be real numbers that satisfy conditions (10) and (12) of Lemma 17. Then we have*

$$(\lceil 1/\varepsilon \rceil \delta N, N) \cap \mathbb{Z} \subseteq \sum_{3 \lceil 1/\varepsilon \rceil} B.$$

Proof. By Lemma 17 (10) and (12), we have that

$$|(B+1) \cap [1, l]| \geq \sum_{i=0}^{l-1} x_i \geq l\varepsilon$$

for any $l \in [N\delta, N]$. Let k_0 be the largest integer such that $|(B+1) \cap [1, k_0]| < k_0\varepsilon$. So we have

- (1) $k_0 < \delta N$.
- (2) For any $k_0 < l \leq N$ we have $|(B+1) \cap [k_0+1, l]| = |(B+1) \cap [1, l]| - |(B+1) \cap [1, k_0]| \geq (l - k_0)\varepsilon$.
- (3) The above property for $l = k_0 + 1$, implies that $k_0 \in B$.

Let $X := \{b - k_0 + 1 \mid b \in B, b \geq k_0 - 1\} \cup \{k \in \mathbb{Z} \mid k \geq N - k_0\}$. By the above properties we have that $\sigma(X) \geq \varepsilon$. Therefore by Mann's theorem (Theorem 19) we have

$$\mathbb{Z}^{\geq 0} = \sum_{\lceil 1/\varepsilon \rceil} (X \cup \{0\}).$$

So for any integer $\lceil 1/\varepsilon \rceil \delta N < m < N$ there are $t \leq \lceil 1/\varepsilon \rceil$ elements of X that add up to $m - \lceil 1/\varepsilon \rceil k_0$. Since $m - \lceil 1/\varepsilon \rceil k_0 < N - k_0$, there are $b_1, \dots, b_t \in B \cap [k_0, \infty)$ such that

$$(b_1 - k_0 + 1) + \dots + (b_t - k_0 + 1) = m - \lceil 1/\varepsilon \rceil k_0.$$

Thus we have

$$m = b_1 + \dots + b_t + (\lceil 1/\varepsilon \rceil - t)k_0 + t \in \sum_{3 \lceil 1/\varepsilon \rceil} B,$$

as $k_0, 0, 1 \in B$.

□

For $\{x_k\}$ as in (9), let

$$(15) \quad T := \{k \in [0, N-1] \mid x_k \geq 1/2\}.$$

In particular, $T \subseteq B$. Here is the main property of the sets B and T .

Lemma 21. *Suppose $k \in B$. Then*

$$D_T(k) \leq 2N \left(\delta + \frac{\log 2}{\log |\mathfrak{f}|} \right),$$

where $D_T(k) := |(T \cap [0, N-1-k]) \setminus (T-k)| = |(T+k \cap [0, N-1]) \setminus T|$.

Proof. Suppose $i \in (T \cap [0, N-1-k]) \setminus (T-k)$. Then

$$(16) \quad \min(x_i, 1 - x_{i+k}) \geq 1/2.$$

On the other hand, since $k \in B$, $x_k \neq 0$. Therefore by Lemma 17 (13) we have

$$\begin{aligned} \frac{D_T(k)}{2} &= \frac{|(T \cap [0, N-1-k]) \setminus (T-k)|}{2} \\ &\leq \sum_{i \in (T \cap [0, N-1-k]) \setminus (T-k)} \min(x_i, 1 - x_{i+k}) \\ &\leq \sum_{j=0}^{N-k-1} \min(x_j, 1 - x_{j+k}) \\ &\leq N \left(\delta + \frac{\log 2}{\log |\mathfrak{f}|} \right). \end{aligned}$$

□

Lemma 22. [LV] *For any positive integers $k_1, k_2 < N$ we have $D_T(k_1 + k_2) \leq D_T(k_1) + D_T(k_2)$.*

Proof. For any three sets A, B , and C we have $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$. Therefore

$$\begin{aligned} D_T(k_1 + k_2) &= |(T \cap [0, N-1-k_1-k_2]) \setminus (T-k_1-k_2)| \\ &\leq |(T \cap [0, N-1-k_1-k_2]) \setminus ((T-k_1) \cap [0, N-1-k_1-k_2])| \\ &\quad + |((T-k_1) \cap [0, N-1-k_1-k_2]) \setminus (T-k_1-k_2)| \\ &\leq D_T(k_1) + D_T(k_2). \end{aligned}$$

□

Lemma 23. [LV] *For some universal implied constants we have*

$$\frac{1}{N} \sum_{k=0}^{N-1} D_T(k) \geq N\varepsilon^3/16$$

if $0 < \varepsilon \ll 1$, $\delta \ll \varepsilon^2$ and $1 \ll_\varepsilon |\mathfrak{f}|$.

Proof. By Lemma 17 (13) we have

$$(17) \quad N \left(\delta + \frac{\log 2}{\log |\mathfrak{f}|} \right) \geq \sum_{i=0}^{N-1} \min(x_i, 1 - x_i) \geq \sum_{i \in [0, N-1] \setminus T} x_i.$$

By Lemma 17 (12), for any integer $l \in [N\delta, N]$, we have

$$l\varepsilon \leq \sum_{i=0}^{l-1} x_i \leq \sum_{i \in [0, N-1] \setminus T} x_i + |T \cap [0, l-1]|.$$

Hence by (17) we have

$$|T \cap [0, l-1]| \geq l \left(\varepsilon - \frac{N}{l} \left(\delta + \frac{\log 2}{\log |f|} \right) \right).$$

Suppose $\delta < \varepsilon^2/16$ and $\log 2/(16\varepsilon^2) < \log |f|$. Then we have

$$(18) \quad |T \cap [0, N\varepsilon/4 - 1]| \geq N\varepsilon^2/8.$$

For any $i \in [N\varepsilon/4 - 1, N - 1]$ and any $k \in T \cap [0, N\varepsilon/4 - 1]$ we have $i \in (T \cap [0, N\varepsilon/4 - 1]) + (i - k)$. Hence for any integer $i \in [N\varepsilon/4 - 1, N - 1]$ we have

$$\sum_{j=0}^{N(1-\varepsilon/4)} \mathbb{1}_{(T \cap [0, N\varepsilon/4 - 1] + j) \setminus T}(i) \geq |T \cap [0, N\varepsilon/4 - 1]| \mathbb{1}_{[0, N-1] \setminus T}(i).$$

By adding over i in the above range we get

$$(19) \quad \sum_{j=0}^{N(1-\varepsilon/4)} D_T(j) \geq |T \cap [0, N\varepsilon/4 - 1]| \cdot |[N\varepsilon/4 - 1, N - 1] \setminus T|.$$

By Lemma 17 (13) we have

$$N \left(\delta + \frac{\log 2}{\log |f|} \right) \geq \sum_{i=0}^{N-1} \min(x_i, 1 - x_i) \geq \sum_{i \in T} (1 - x_i) \geq |T| - \sum_{i=0}^{N-1} x_i \geq |T| - (1 - \varepsilon)N$$

Therefore, since by our assumption $\delta < \varepsilon^2/16$ and $\log 2/(16\varepsilon^2) < \log |f|$, we have

$$(20) \quad |T| \leq N(1 - \varepsilon + \varepsilon^2/8).$$

Hence by (18), (19), and (20) we have

$$\sum_{j=0}^{N-1} D_T(j) \geq N(\varepsilon^2/8) \cdot N(3\varepsilon/4 - \varepsilon^2/8) \geq N^2\varepsilon^3/16.$$

□

Corollary 24. *For some integer $j_0 \in [N\varepsilon^3/32, N - 1]$, we have $D_T(j_0) \geq N\varepsilon^3/32$ if $0 < \varepsilon \ll 1$, $\delta \ll \varepsilon^2$ and $1 \ll_\varepsilon |f|$.*

Proof. By Lemma 23 we have

$$\sum_{j \in [N\varepsilon^3/32, N-1]} D_T(j) \geq \sum_{i=0}^{N-1} D_T(j) - (N\varepsilon^3/32)(N) \geq N^2\varepsilon^3/16 - N^2\varepsilon^3/32 = N^2\varepsilon^3/32.$$

And so for some $j_0 \in [N\varepsilon^3/32, N - 1]$ we have $D_T(j_0) \geq N\varepsilon^3/32$. □

Proof of Proposition 16. Suppose $\delta < \varepsilon^4/512$, $512(\log 2)\varepsilon^{-4} < \log |f|$, and for some A the assertion of Proposition 16 does not hold. Then we consider B and T as above. Hence by Corollary 24 we have

$$D_T(j_0) \geq N\varepsilon^3/32$$

for some integer $j_0 \in [N\varepsilon^3/32, N - 1]$. On the other hand, by Lemma 20, since $j_0 \geq N\varepsilon^3/32 > N[1/\varepsilon]\delta$, there are at most $3[1/\varepsilon]$ elements b_1, \dots, b_t of B such that

$$j_0 = b_1 + \dots + b_t.$$

Hence by Lemma 22,

$$(21) \quad D_T(b_i) > N\varepsilon^4/100$$

for some i .

On the other hand, by Lemma 21, we have that for any $b \in B$

$$D_T(b) \leq 2N \left(\delta + \frac{\log 2}{\log |\mathfrak{f}|} \right) < N\varepsilon^4/128,$$

which contradicts (21). \square

2.3. Proof of Theorem 5: Scalar-Sum-Product expansion. As in [BG09] (also see [Bor08] or [SG-a, Section 2.3]), we start by a regularization process. The \mathfrak{p} -adic filtration $\{\pi_{\mathfrak{p}^N}(\mathfrak{p}^i \mathcal{O})\}_{i=1}^N$ induces an $|\mathfrak{f}|$ -regular rooted tree structure (with N -levels) on $\pi_{\mathfrak{p}^N}(\mathcal{O})$. So by a similar argument as the above mentioned articles we get the following large regular subset of A .

Lemma 25. *Let $0 < \delta < \varepsilon < 1$ and $|\mathfrak{f}| \gg_{\varepsilon, \delta} 1$. Then for $0 < \delta' \leq \varepsilon\delta/4$ the following holds: Let $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$. Suppose that A satisfies the following properties:*

- (1) $|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon}$ for any $N\delta' \leq i \leq N$,
- (2) $|A + A| \geq |A||\mathfrak{f}|^{N\delta'}$.

Then there is $A' \subseteq A$ such that

- (1) A' is (m_0, \dots, m_{N-1}) -regular.
- (2) $|A'| \geq |A|/(2 \log |\mathfrak{f}|)^N$.
- (3) $|\pi_{\mathfrak{p}^i}(A')| \geq |\mathfrak{f}|^{i\varepsilon/2}$ for $N\delta \leq i \leq N$.

Proof. By [SG-a, Section 2.3], there is a subset $A' \subseteq A$ such that $|A'| \geq |A|/(2 \log |\mathfrak{f}|)^N$ and A' is an (m_0, \dots, m_{N-1}) -regular set. Let $\bar{n} := \max\{i \in [0, N-1] \mid |\pi_{\mathfrak{p}^i}(A')| < |\mathfrak{f}|^{i\varepsilon/2}\}$. To show that A' satisfies the above three conditions, it is enough to show that, if $0 < \delta' \leq \varepsilon\delta/4$ and $|\mathfrak{f}| \gg_{\varepsilon, \delta} 1$, then $\bar{n} < N\delta$.

Suppose to the contrary that $\bar{n} \geq N\delta > N\delta'$. Then by the assumption $|\pi_{\mathfrak{p}^{\bar{n}}}(A')| \geq |\mathfrak{f}|^{\bar{n}\varepsilon}$. On the other hand, there is a subset $A'' \subseteq A'$ such that $|\pi_{\mathfrak{p}^{\bar{n}}}(A'')| = 1$ and

$$|A''| = \frac{|A'|}{|\pi_{\mathfrak{p}^{\bar{n}}}(A')|} > \frac{|A|}{(2 \log |\mathfrak{f}|)^N |\mathfrak{f}|^{\bar{n}\varepsilon/2}}.$$

Therefore we have

$$|A||\mathfrak{f}|^{N\delta'} \geq |A + A| \geq |A''||\pi_{\mathfrak{p}^{\bar{n}}}(A)| \geq \frac{|A||\mathfrak{f}|^{\bar{n}\varepsilon}}{(2 \log |\mathfrak{f}|)^N |\mathfrak{f}|^{\bar{n}\varepsilon/2}},$$

which implies that

$$(22) \quad (2 \log |\mathfrak{f}|)^N \geq |\mathfrak{f}|^{\bar{n}\varepsilon/2 - N\delta'} \geq |\mathfrak{f}|^{N(\delta\varepsilon/2 - \delta')} \geq |\mathfrak{f}|^{N(\delta\varepsilon/4)}.$$

For $|\mathfrak{f}| \gg_{\varepsilon, \delta} 1$ (so that $2 \log |\mathfrak{f}| < |\mathfrak{f}|^{\delta\varepsilon/8}$), (22) implies that $\varepsilon/8 \geq \varepsilon/4$, which is a contradiction. \square

Proof of Theorem 5. Let $\delta_r(\varepsilon/2)$ (r stands for regular) be such that $0 < \delta_r(\varepsilon/2) \ll (\varepsilon/2)^4$ where the implied constant is given by Proposition 16. Suppose $|\mathfrak{f}| \gg_{\varepsilon} 1$, where the implied constant is given by Lemma 25 for $\varepsilon/2$ and $\delta_r(\varepsilon/2)$. Now let $\delta' \ll (\varepsilon/2)\delta_r(\varepsilon/2)$ be given by Lemma 25.³ We claim δ' satisfies the desired conditions.

By the choice of δ' and Lemma 25, there is $A' \subseteq A$ such that

- (1) $|A'|$ is an (m_0, \dots, m_{N-1}) -regular subset.
- (2) $|\pi_{\mathfrak{p}^i}(A')| \geq |\mathfrak{f}|^{i\varepsilon/2}$ for $N\delta_r(\varepsilon/2) \leq i \leq N$,
- (3) $|A'| \geq |A|/(2 \log |\mathfrak{f}|)^N$.

³To avoid further confusion with the δ used in Lemma 25, we are using δ' , here. This is, in fact, supposed to be the claimed δ in Theorem 5.

Next we modify A' a bit, if necessary, to make sure that m_0 and m_1 are at least 2.

If $m_0 = 1$ and $m_1 > 1$, then $A' + \{a_{01}, a_{02}\}$ is a $(2, m_1, \dots, m_{N-1})$ -regular subset of $A + A$.

If $m_0 = m_1 = 1$, then $A' + \{a_{11}, a_{12}\} + \{a_{01}, a_{12}\}$ is a $(2, 2, m_2, \dots, m_{N-1})$ -regular subset of $A + A + A$.

If $m_0 > 1$ and $m_1 = 1$, then

- (1) there is a subset X_0 of A such that $|X_0| = |\pi_p(X_0)| = |\pi_p(A)|$,
- (2) there is a $(1, 1, m_2, \dots, m_{N-1})$ -regular subset A'_0 of A'

Then $A'_0 + \{a_{11}, a_{12}\} + X_0$ is a regular $(|\pi_p(A)|, 2, m_2, \dots, m_{N-1})$ -regular subset of $A + A + A$.

So in all the cases we get an (m_0, \dots, m_{N-1}) -regular subset A' of $A + A + A$ such that

- (1) $m_0, m_1 > 1$.
- (2) $|\pi_{p^i}(A')| \geq |\mathfrak{f}|^{i\varepsilon/2}$ for $N\delta_r(\varepsilon/2) \leq i \leq N$.
- (3) $|A'| \geq |A|/(2 \log |\mathfrak{f}|)^N$.

If $|\langle A \rangle_6| \geq |A||\mathfrak{f}|^{N\delta}$ (for small enough δ to be determined later), we are done. So suppose this does not hold. In particular, $|A + A + A| \leq |A||\mathfrak{f}|^{N\delta}$. Hence $|A + A + A| \leq |\mathfrak{f}|^{N(1-\varepsilon+\delta)}$. So assuming $\delta < \varepsilon/2$, we have that $|A'| \leq |\mathfrak{f}|^{N(1-\varepsilon/2)}$. Hence A' satisfies all the conditions of Proposition 16. Therefore we have

$$(23) \quad \max_{\omega \in \Omega, x \in A' - A'} |A' + \pi_{p^N}(\omega)x A'| \geq |A'| |\mathfrak{f}|^{N\delta_r(\varepsilon/2)}.$$

Since at least one of a_{01}, a_{02} is a unit, we have that

$$|\langle A \rangle_6 + \pi_{p^N}(\omega)\langle A \rangle_6| \geq |A' + \pi_{p^N}(\omega)x A'|.$$

Therefore we have

$$\max_{\omega \in \Omega} |\langle A \rangle_6 + \pi_{p^N}(\omega)\langle A \rangle_6| \geq |A'| |\mathfrak{f}|^{N\delta_r(\varepsilon/2)} \geq |A| \left(\frac{|\mathfrak{f}|^{\delta_r(\varepsilon/2)}}{2 \log |\mathfrak{f}|} \right)^N.$$

Suppose $|\mathfrak{f}| \gg_\varepsilon 1$ so that $|\mathfrak{f}|^{\delta_r(\varepsilon/2)/2} \geq 2 \log |\mathfrak{f}|$. Hence we get

$$\max_{\omega \in \Omega} |\langle A \rangle_6 + \pi_{p^N}(\omega)\langle A \rangle_6| \geq |A| |\mathfrak{f}|^{N\delta_r(\varepsilon/2)/2} \geq |A| |\mathfrak{f}|^{N\delta'}.$$

□

2.4. Proof of Theorem 6: a scalar-sum-product set contains a large congruence set.

Proposition 26. *For any $0 < \varepsilon_1 \ll \varepsilon_2 \ll 1$, $0 < \delta \ll \varepsilon_1^5$, and positive integer $1 \ll_{\varepsilon_1} C$, and any finite extension K of \mathbb{Q}_p with large, depending on ε_1 , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Let $\Omega \subseteq \mathcal{O}$, and suppose π_p induces a bijection between $\Omega \subseteq \mathcal{O}$ and \mathfrak{f}^\times . Suppose $A \subseteq \pi_{p^N}(\mathcal{O})$ such that

- (1) $|\pi_{p^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon_1}$ for any $N\delta \leq i \leq N$.
- (2) *there are $a_{01}, a_{02}, a_{11}, a_{12} \in A$ such that $a_{i1} - a_{i2} \in \pi_{p^N}(\mathfrak{p}^i \mathcal{O} \setminus \mathfrak{p}^{i+1} \mathcal{O})$.*

Then

$$\pi_{p^N}(\mathfrak{p}^{\lceil \varepsilon_2 N \rceil} \mathcal{O}) \subseteq \langle A \rangle_C + \pi_{p^N}(\omega_1)\langle A \rangle_C + \dots + \pi_{p^N}(\omega_C)\langle A \rangle_C,$$

for some $\omega_i \in \prod_C(\Omega \cup \{1\})$.

Proof of Theorem 6 modulo Proposition 26. Let $\delta \ll \varepsilon_1^{5m}$. Hence by Proposition 26 applied to the set $\pi_{p^{N_m}}(A)$, where $N_m := \lfloor \varepsilon_2^{m-1} N \rfloor$, we get that for a positive integer $1 \ll_{\varepsilon_1} k$ there are $\omega_i \in \prod_k(\Omega \cup \{1\})$

such that

$$\begin{aligned}
 \pi_{\mathfrak{p}^{N_m}}(\mathfrak{p}^{\lceil \varepsilon_2^m N \rceil} \mathcal{O}) &\subseteq \pi_{\mathfrak{p}^{N_m}}(\mathfrak{p}^{\varepsilon_2 N_m} \mathcal{O}) \\
 &\subseteq \langle \pi_{\mathfrak{p}^{N_m}}(A) \rangle_k + \pi_{\mathfrak{p}^{N_m}}(\omega_1) \langle \pi_{\mathfrak{p}^{N_m}}(A) \rangle_k + \cdots + \pi_{\mathfrak{p}^{N_m}}(\omega_k) \langle \pi_{\mathfrak{p}^{N_m}}(A) \rangle_k \\
 (24) \quad &\subseteq \pi_{\mathfrak{p}^{N_m}}(\langle A \rangle_k + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_k + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \langle A \rangle_k),
 \end{aligned}$$

For any $1 \leq j \leq \varepsilon_2^{-m}$, since $N\delta \leq j\varepsilon_2^m N \leq N$, by our assumption there is $x_j \in A - A$ such that

$$x_j \in \mathfrak{p}^{\lfloor j\varepsilon_2^m N \rfloor} \pi_{\mathfrak{p}^N}(\mathcal{O}) \setminus \mathfrak{p}^{\lfloor j\varepsilon_2^m N \rfloor + 1} \pi_{\mathfrak{p}^N}(\mathcal{O}).$$

Hence by (24) we have

$$\begin{aligned}
 \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon_2^m N \rceil} \mathcal{O}) &\subseteq \langle A \rangle_k + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_k + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \text{gen} A k \\
 &\quad + x_1(\langle A \rangle_k + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_k + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \langle A \rangle_k) \\
 &\quad + \cdots \\
 &\quad + x_{\lceil \varepsilon_2^{-m} \rceil}(\langle A \rangle_k + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_k + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \langle A \rangle_k).
 \end{aligned}$$

And, since A contains a unit and $\varepsilon_1 \leq \varepsilon_2$, we have that for a positive integer $1 \ll_{m, \varepsilon_1} C$

$$\pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon_2^m N \rceil} \mathcal{O}) \subseteq \langle A \rangle_C + \pi_{\mathfrak{p}^N}(\omega_1) \langle A \rangle_C + \cdots + \pi_{\mathfrak{p}^N}(\omega_k) \langle A \rangle_C$$

□

To prove Proposition 26, let us start with a direct corollary of [BG09, Lemma A.1].

Lemma 27. *Let K be a finite extension of \mathbb{Q}_p , \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Suppose $B \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that for any $1 \leq k \leq N$,*

$$\max_{\xi} |\{x \in B \mid \pi_{\mathfrak{p}^k}(x) = \xi\}| < |\mathfrak{f}|^{-(3/4)k} |B|.$$

Then $\langle B \rangle_{200} = \pi_{\mathfrak{p}^N}(\mathcal{O})$.

Proof. It is a consequence of [BG09, Lemma A.1] as it is observed in [BG09, Proof of Corollary A.1]. □

Next following [BG09, Proof of Corollary A.1] we show how Lemma 27 helps us to deal with (extremely) large sets.

Lemma 28. *For any $0 < \varepsilon \ll 1$, $0 < \delta \ll \varepsilon$, and any finite extension K of \mathbb{Q}_p the following holds:*

Let \mathcal{O} be the ring of integers of K , \mathfrak{p} be a uniformizing element of K , and \mathfrak{f} be the residue field. Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that $|A| \geq |\mathfrak{f}|^{N(1-\delta)}$. Then

$$\pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil} \mathcal{O}) \subseteq \langle A \rangle_{200}.$$

Proof. ⁴ Let

$$n_0 := \max\{k \mid \max_{\xi} |\{x \in A \mid \pi_{\mathfrak{p}^k}(x) = \xi\}| > |\mathfrak{f}|^{-(3/4)k} |A|\}.$$

Hence for small enough δ (to be determined later) we have

$$|\mathfrak{f}|^{N-n_0} > |\mathfrak{f}|^{-(3/4)n_0} |A| \geq |\mathfrak{f}|^{-(3/4)n_0} |\mathfrak{f}|^{N(1-\delta)}.$$

Therefore we have

$$(25) \quad n_0 < 4N\delta.$$

Let $\xi \in \pi_{\mathfrak{p}^{n_0}}(\mathcal{O})$ be such that $A' := \{x \in A \mid \pi_{\mathfrak{p}^{n_0}}(x) = \xi\}$ has at least $|\mathfrak{f}|^{-(3/4)n_0} |A|$ -many elements. And let

$$B := \pi_{\mathfrak{p}^{N-n_0}}(\{x \in \mathcal{O} \mid \pi_{\mathfrak{p}^N}(x_0 + \mathfrak{p}^{n_0}x) \in A'\}),$$

⁴This is identical to [BG09, Proof of Corollary A.1]. It is included for the convenience of the reader.

where $\pi_{\mathfrak{p}^{n_0}}(x_0) = \xi$. By Lemma 27, we have that

$$\langle B \rangle_{200} = \pi_{\mathfrak{p}^{N-n_0}}(\mathcal{O}).$$

Hence

$$\langle A \rangle_{200} \supseteq \pi_{\mathfrak{p}^N}(\mathfrak{p}^{200n_0}\mathcal{O}).$$

Now (25) gives us the claim. \square

Proof of Proposition 26. By Lemma 28, it is enough to prove that

$$(26) \quad |\langle A \rangle_C + \pi_{\mathfrak{p}^N}(\omega_1)\langle A \rangle_C + \cdots + \pi_{\mathfrak{p}^N}(\omega_C)\langle A \rangle_C| \geq |\mathfrak{f}|^{N(1-O(\varepsilon_2))},$$

for a positive integer $C \gg_{\varepsilon_1} 1$ and $\omega_i \in \prod_C(\Omega \cup \{1\})$. One can get (26) by applying Theorem 5 repeatedly and using the fact that $\varepsilon_1 \ll \varepsilon_2$. \square

3. GETTING A THICK \mathbb{Z}_p -SEGMENT IN A SUM-PRODUCT OF A LARGE SET.

In this section, first using a \mathfrak{p} -adic version of the method of the proof of [BKT04] for the sets with non-zero *graded structures* we will get a *thick \mathbb{Z}_p -segment* in a sum-product set. Then the general case will be reduced to this case using another application of Mann's theorem.

3.1. The case of non-zero graded structures. In this section we essentially modify the argument given in [BKT04] for the \mathfrak{p} -adic setting.

Proposition 29. *For any $0 < \varepsilon_1 \ll \varepsilon_2 \ll 1$, $0 < \delta \ll_{\varepsilon_1} 1$, and positive integers $1 \ll_{\varepsilon_1} C$ and e_0 , and any finite extension K of \mathbb{Q}_p with large, depending on ε_1 , residue field \mathfrak{f} the following holds:*

Let \mathcal{O} be the ring of integers of K , and \mathfrak{p} be a uniformizing element of K . Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ such that

- (1) $|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon_1}$ for any $N\delta \leq i \leq N$.
- (2) $\text{gr}_{e_0 i}(A) \neq 0$ for any $N\delta \leq e_0 i \leq N$, where $\text{gr}_j(X) := \pi_{\mathfrak{p}}(\{x \in \mathcal{O} \mid \pi_{\mathfrak{p}^N}(\mathfrak{p}^j x) \in X\})$.
- (3) $0, 1 \in A$ and there are $a_1, a_2 \in A$ such that $a_1 - a_2 \in \pi_{\mathfrak{p}^N}(\mathfrak{p}\mathcal{O} \setminus \mathfrak{p}^2\mathcal{O})$.

Then

$$\pi_{\mathfrak{p}^{\lfloor 2\varepsilon' N \rfloor}}(\mathfrak{p}^{e_0 \lceil \varepsilon' N / e_0 \rceil} \mathbb{Z}x) \subseteq \pi_{\mathfrak{p}^{\lfloor 2\varepsilon' N \rfloor}}(\langle A \rangle_C),$$

for some $\varepsilon_2^{m(\varepsilon_1)} \leq \varepsilon' \leq \varepsilon_2$, and $x \in \mathcal{O}$.

Proof. Let $m := m(\varepsilon_1)$ be a large integer (will be determined later). By Hensel's lemma, we know that there is a subgroup Ω of \mathcal{O}^\times such that $\pi_{\mathfrak{p}}$ induces an isomorphism between Ω and \mathfrak{f}^\times . Let $\psi_{0,N}$ be as in the paragraph of (1). Then by Theorem 6, if $0 < \delta \ll_{\varepsilon_1, m} 1$, we have that

$$(27) \quad \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon_2^m N \rceil} \mathcal{O}) \subseteq \langle A \rangle_{C_1} + \psi_{0,N}(\alpha_1)\langle A \rangle_{C_1} + \cdots + \psi_{0,N}(\alpha_k)\langle A \rangle_{C_1},$$

for some integers $k := k(\varepsilon_1)$ and $C_1 := C_1(\varepsilon_1, m)$, and $\alpha_i \in \mathfrak{f}^\times$.

Now we introduce a process through which the number k of the involved scalars will be reduced in the expense of enlarging C_1 and shrinking the size of the congruence subgroup, i.e. enlarging ε_2^m . Then we will analyze the case when this process halts before getting $k = 0$.

For simplicity we say $\text{BG}(A; \varepsilon, k, C)$ holds if for k elements $\alpha_i \in \mathfrak{f}^\times$ we have

$$(28) \quad \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil} \mathcal{O}) \subseteq \langle A \rangle_C + \psi_{0,N}(\alpha_1)\langle A \rangle_C + \cdots + \psi_{0,N}(\alpha_k)\langle A \rangle_C.$$

Claim 1. *Suppose $0 < \delta_0 < 1$ and $\text{BG}(A; \varepsilon, k, C)$ holds. Then we have either (**reduction**)*

$$(29) \quad \text{BG}(A; \varepsilon + \delta_0, k - 1, 8C),$$

*or (**δ_0 -injectivity**) for any $\mathbf{x}, \mathbf{x}' \in \langle A \rangle_{2C}^{k+1} := \langle A \rangle_{2C} \times \cdots \times \langle A \rangle_{2C}$ we have that*

$$(30) \quad l(\mathbf{x}) = l(\mathbf{x}') \Rightarrow \mathbf{x} - \mathbf{x}' \in \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lfloor \delta_0 N \rfloor}),$$

where $l(x_0, \dots, x_k) := x_0 + \psi_{0,N}(\alpha_1)x_1 + \dots + \psi_{0,N}(\alpha_k)x_k$ and $\alpha_i \in \mathfrak{f}^\times$ satisfy (28).

Proof of Claim 1. Suppose δ_0 -injectivity fails, i.e. there are $\mathbf{x}, \mathbf{x}' \in \langle A \rangle_{2C} \times \dots \times \langle A \rangle_{2C}$ such that

- (1) $\mathbf{x} - \mathbf{x}' \notin \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lfloor \delta_0 N \rfloor} \mathcal{O})^{k+1}$, and
- (2) $l(\mathbf{x}) = l(\mathbf{x}')$.

Then, for some i_0 , $(x_{i_0} - x'_{i_0})\pi_{\mathfrak{p}^N}(\mathcal{O}) \supseteq \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lfloor \delta_0 N \rfloor} \mathcal{O})$. Without loss of generality let us assume that it happens for $i_0 = k$ (notice that, if $i_0 = 0$, we can multiply both sides by $\psi_{0,N}(\alpha_1^{-1})$ to make sure that one of the remaining coefficients is one). Hence we have

$$\begin{aligned} \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil + \lfloor \delta_0 N \rfloor} \mathcal{O}) &\subseteq \psi_{0,N}(\alpha_0) \langle A \rangle_{2C}(x_k - x'_k) + \dots + \psi_{0,N}(\alpha_k) \langle A \rangle_{2C}(x_k - x'_k) \\ (\text{since } l(\mathbf{x}) = l(\mathbf{x}'),) &\subseteq \psi_{0,N}(\alpha_0) \langle A \rangle_{4C} + \dots + \psi_{0,N}(\alpha_{k-1}) \langle A \rangle_{4C} - \left(\sum_{i=0}^{k-1} \psi_{0,N}(\alpha_i)(x_i - x'_i) \right) \langle A \rangle_{2C} \\ (31) \quad &\subseteq \psi_{0,N}(\alpha_0) \langle A \rangle_{8C} + \dots + \psi_{0,N}(\alpha_{k-1}) \langle A \rangle_{8C}, \end{aligned}$$

which means that $\text{BG}(A; \varepsilon + \delta_0, k-1, 8C)$ holds. \square

Claim 2. Suppose $\text{BG}(A; \varepsilon, k, C)$ holds and $\alpha_i \in \mathfrak{f}^\times$ satisfy (28). If $l(\mathbf{x}) := \sum_i \alpha_i x_i$ is δ_0 -injective on $\langle A \rangle_{2C}^{k+1}$ for some $\delta_0 > \varepsilon$ (see (30)), then

$$\pi_{\mathfrak{p}^{\lfloor \delta_0 N \rfloor}} \left(\langle A \rangle_C \cap \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil} \mathcal{O}) \right)$$

is closed under addition.

Proof of Claim 2. Let $x, x' \in \langle A \rangle_{2C} \cap \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil} \mathcal{O})$. So there is $\mathbf{x} \in \langle A \rangle_C \times \dots \times \langle A \rangle_C$ such that $l(\mathbf{x}) = x + x' = l(x + x', 0, \dots, 0)$.

By assumption for any $\mathbf{x}, \mathbf{x}' \in \langle A \rangle_{2C} \times \dots \times \langle A \rangle_{2C}$ we have that

$$(32) \quad l(\mathbf{x}) = l(\mathbf{x}') \Rightarrow \mathbf{x} - \mathbf{x}' \in \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lfloor \delta_0 N \rfloor} \mathcal{O})^{k+1}.$$

Hence we have

$$\mathbf{x} \equiv (x + x', 0, \dots, 0) \pmod{\mathfrak{p}^{\lfloor \delta_0 N \rfloor}},$$

which implies that $\pi_{\mathfrak{p}^{\lfloor \delta_0 N \rfloor}}(A \cap \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon N \rceil} \mathcal{O}))$ is closed under addition. \square

Having the above Claims, we inductively define three sequence of numbers $\{\varepsilon'_i\}, \{k'_i\}, \{C'_i\}$:

$$\begin{aligned} \varepsilon'_0 &:= \varepsilon_2^m, & \varepsilon'_{i+1} &:= 3\varepsilon'_i; \\ k'_0 &:= k, & k'_{i+1} &:= k_i - 1; \\ C'_0 &:= C_1, & C'_{i+1} &:= 8C'_i. \end{aligned}$$

First notice that for $\varepsilon_2 \ll 1$ and $k(\varepsilon_1) \leq m(\varepsilon_1)$ we have that

$$(33) \quad \varepsilon'_i \leq 3^k \varepsilon_2^m \leq 3^k 3^{-m} \varepsilon_2 \leq \varepsilon_2, \quad C'_i \leq 8^k C_1 \ll_{\varepsilon_1} 1.$$

We know that $\text{BG}(A; \varepsilon'_0, k'_0, C'_0)$ holds. Suppose i_0 is the smallest non-negative integer such that

$$\text{BG}(A; \varepsilon'_{i_0+1}, k'_{i_0+1}, C'_{i_0+1})$$

does not hold. If $i_0 = k$, then $\text{BG}(A; \varepsilon_2, 0, 4^k C_1)$ holds. And we are done. Suppose $i_0 < k$. So, by Claim 1, $\text{BG}(A; \varepsilon'_{i_0}, k'_{i_0}, C'_{i_0})$ holds for some $\alpha_j \in \mathfrak{f}^\times$ and $l(\mathbf{x}) := \sum_j \alpha_j x_j$ is $2\varepsilon'_{i_0}$ -injective on $\langle A \rangle_{2C'_{i_0}}^{k'_{i_0}+1}$. Therefore, by Claim 2,

$$\pi_{\mathfrak{p}^{\lfloor 2\varepsilon'_{i_0} N \rfloor}} \left(\langle A \rangle_{C'_{i_0}} \cap \pi_{\mathfrak{p}^N}(\mathfrak{p}^{\lceil \varepsilon'_{i_0} N \rceil} \mathcal{O}) \right)$$

is closed under addition. Since $\text{gr}_{e_0 \lceil \varepsilon'_{i_0} N / e_0 \rceil}(A) \neq 0$, there is $x \in \mathcal{O}^\times$ such that

$$\pi_{\mathfrak{p}^N}(\mathfrak{p}^{e_0 \lceil \varepsilon'_{i_0} N / e_0 \rceil} x) \in A.$$

Hence $\pi_{\mathfrak{p}^{\lfloor 2\varepsilon'_{i_0} N \rfloor}}(\mathfrak{p}^{e_0 \lceil \varepsilon'_{i_0} N / e_0 \rceil} \mathbb{Z}x) \subseteq \pi_{\mathfrak{p}^{\lfloor 2\varepsilon'_{i_0} N \rfloor}}(\langle A \rangle_{C'_{i_0}})$, which finishes the proof. \square

3.2. Proof of Theorem 1. Let us start with (a variation of) [BKT04, Theorem 4]. We include the proof for the convenience of the reader.

Lemma 30. *For any $0 < \varepsilon \ll 1$, positive integer $C \gg_\varepsilon 1$, and a finite field \mathfrak{f} the following holds:*

Suppose $B \subseteq \mathfrak{f}$, $|B| \geq |\mathfrak{f}|^\varepsilon$, and $0, 1 \in B$. Then $\langle B \rangle_C$ is a subfield of \mathfrak{f} .

Proof. By [BKT04, Lemma 4.1], there are $\alpha_1, \dots, \alpha_k \in \mathfrak{f}^\times$ such that $k \ll_\varepsilon 1$ and

$$\alpha_1 B + \dots + \alpha_k B = \mathfrak{f}.$$

Claim 1: *Suppose $0, 1 \in X \subseteq \mathfrak{f}$ and $\alpha_i \in \mathfrak{f}^\times$ such that*

$$(34) \quad \mathfrak{f} = \alpha_1 X + \dots + \alpha_k X.$$

Then either we have (reduction) $\mathfrak{f} = \sum_{i \neq i_0} \alpha_i \langle X \rangle_2$, for some i_0 , or (injectivity) for any $\mathbf{x}, \mathbf{x}' \in X^k$ $\sum_i \alpha_i x_i = \sum_i \alpha_i x'_i \Rightarrow \mathbf{x} = \mathbf{x}'$.

Proof of Claim. Suppose that the injectivity does not hold, i.e. there are $\mathbf{x} \neq \mathbf{x}' \in X^k$ such that

$$(35) \quad \sum_i \alpha_i x_i = \sum_i \alpha_i x'_i.$$

Without loss of generality we can assume that $x_k \neq x'_k$. Thus

$$\begin{aligned} \mathfrak{f} &= \alpha_1(x_k - x'_k)X + \dots + \alpha_k(x_k - x'_k)X \\ (\text{by (35)}) \quad &\subseteq \alpha_1(X \cdot X - X \cdot X) + \dots + \alpha_{k-1}(X \cdot X - X \cdot X) + \left(\sum_{i=1}^{k-1} \alpha_i(x_i - x'_i) \right) X \\ &\subseteq \alpha_1 \langle X \rangle_2 + \dots + \alpha_{k-1} \langle X \rangle_2. \end{aligned}$$

\square

Claim 2: *Suppose $0, 1 \in X \subseteq \mathfrak{f}$ and $\alpha_i \in \mathfrak{f}^\times$ such that*

$$\mathfrak{f} = \alpha_1 X + \dots + \alpha_k X.$$

Suppose for any $\mathbf{x}, \mathbf{x}' \in \langle X \rangle_2^k$ we have

$$\sum_i \alpha_i x_i = \sum_i \alpha_i x'_i \Rightarrow \mathbf{x} = \mathbf{x}'.$$

Then X is a subfield of \mathfrak{f} .

Proof of Claim. It is enough to show $X \cdot X = X$ and $X + X = X$. For any $y, y' \in X$, there is $\mathbf{x} \in X^k$ such that

$$\alpha_1(y + y') = \sum_i \alpha_i x_i.$$

Hence $y + y' = x_1 \in X$. And so X is closed under addition. Similarly it is closed under multiplication. \square

Now suppose $i_0 \leq k$ be the largest non-negative integer such that

$$\mathfrak{f} = \alpha'_1 \langle B \rangle_{4^{i_0}} + \cdots + \alpha'_{k-i_0} \langle B \rangle_{4^{i_0}},$$

for some $\alpha'_i \in \mathfrak{f}^\times$. If $i_0 = k$, we are done. If not, then by Claim 1 for $X = \langle \langle B \rangle_{4^{i_0}} \rangle_2$ we have that for any $\mathbf{x}, \mathbf{x}' \in \langle \langle B \rangle_{4^{i_0}} \rangle_2^{k-i_0}$ we have

$$\sum_i \alpha'_i x_i = \sum_i \alpha'_i x'_i \Rightarrow \mathbf{x} = \mathbf{x}'.$$

Hence, by Claim 2, $\langle B \rangle_{4^{i_0}}$ is a subfield of \mathfrak{f} . □

Lemma 31. *For any $0 < \varepsilon \ll 1$, positive integer e , positive integers $1 \ll_{\varepsilon, e} C, N$, and any finite extension K of \mathbb{Q}_p with large enough, depending on ε , residue field and ramification index at most e , the following holds:*

Suppose $A \subseteq \pi_{\mathfrak{p}^N}(\mathcal{O})$ is an (m_0, \dots, m_{N-1}) -regular set such that

$$|\pi_{\mathfrak{p}^i}(A)| \geq |\mathfrak{f}|^{i\varepsilon}$$

for any $1 \leq i \leq N$. Then

$$\{i \in \mathbb{Z} \mid 0 \leq i \leq N-1, \text{gr}_i(\langle A \rangle_C) \neq 0\} \supseteq [0, N-1] \cap e_0 \mathbb{Z},$$

for some positive integer $e_0 \leq e$.

Proof. For any subset X of $\pi_{\mathfrak{p}^N}(\mathcal{O})$, let

$$J(X) := \{k \in \mathbb{Z} \mid k \geq 0, \text{gr}_k(X) \neq 0\}.$$

Notice that $J(X_1) + J(X_2) \subseteq J(X_1 X_2)$. For any $\lambda \in \mathcal{O}^\times$, $J(\lambda X) = J(X)$, and $\langle \lambda X \rangle_C = \lambda^C \langle X \rangle_C$. On the other hand, since $|\pi_{\mathfrak{p}}(A)| \geq |\mathfrak{f}|^\varepsilon > 1$, A contains a unit. Hence we can and will replace A with $\lambda(A - A)$ for some λ and assume $0, 1 \in A$ and it contains an (m_0, \dots, m_{N-1}) -regular subset A' . Now, by Lemma 30, if $C_1 \gg_\varepsilon 1$, then $\pi_{\mathfrak{p}}(\langle A \rangle_{C_1})$ is a subfield of \mathfrak{f} . Since any subfield is of characteristic p , it cannot be embedded into $\mathcal{O}/\mathfrak{p}^{e+1}\mathcal{O}$ where e is the ramification index of K over \mathbb{Q}_p . Hence

$$e_0 := \min(J(\langle A \rangle_{2C_1}) \setminus \{0\}) \leq e.$$

Let's observe that

$$(36) \quad \sum_{e_0} J(\langle A \rangle_{2C_1}) \supseteq \{e_0\} \cup e_0 J(\langle A \rangle_{2C_1}).$$

Hence we have

$$(37) \quad J := \{j \in \mathbb{Z} \mid j \geq 0, e_0 j \in \sum_{e_0} J(\langle A \rangle_{2C_1})\} \supseteq \{1\} \cup J(\langle A \rangle_{2C_1}).$$

Let $x_i := \frac{\log m_i}{\log |\mathfrak{f}|}$. Then $0 \leq x_j \leq 1$, and, if $x_j \neq 0$, then $j \in J(A - A) \subseteq J$. By the assumption, we have

$$(38) \quad \sum_{j=0}^l x_j \geq l\varepsilon,$$

for any $0 \leq l \leq N-1$. By (37) and (38), for any positive integer k , we have

$$|(J \cup \mathbb{Z}^{\geq N}) \cap [1, k]| \geq \max\{k\varepsilon - 1, 1\} \geq k\varepsilon/2.$$

This implies that the Schnirelmann density $\sigma(J \cup \mathbb{Z}^{\geq N}) \geq \varepsilon/2$. Hence by Mann's Theorem (Theorem 19) we have

$$(39) \quad [0, N-1] \cap \mathbb{Z} \subseteq \sum_{\lceil 2/\varepsilon \rceil} J.$$

Hence, by (36) and (39), we have

$$[0, N-1] \cap e_0 \mathbb{Z} \subseteq \sum_{e_0 \lceil 2/\varepsilon \rceil} J(\langle A \rangle_{2C_1}) \subseteq J(\langle A \rangle_{2e_0 \lceil 2/\varepsilon \rceil C_1}).$$

□

Proof of Theorem 1. As in [BG09] (see also [SG-a, Section 2.3]), there is $A' \subseteq A$ such that $\pi_{\mathfrak{p}^N}(A')$ is an (m_0, \dots, m_{N-1}) -regular set, and

$$|\pi_{\mathfrak{p}^N}(A')| \geq \frac{|A|}{(2 \log |\mathfrak{f}|)^N} \geq |\mathfrak{f}|^{N\varepsilon/2},$$

for $|\mathfrak{f}| \gg_\varepsilon 1$. Let

$$\bar{n} := \max\{k \mid |\pi_{\mathfrak{p}^k}(A')| = m_0 \cdots m_{k-1} < |\mathfrak{f}|^{k\varepsilon/4}\}.$$

So for any $\bar{n} + 1 \leq l \leq N$, we have

$$(40) \quad \prod_{i=\bar{n}}^{l-1} m_i \geq \left(\prod_{i=0}^{l-1} m_i \right) \left(\prod_{i=0}^{\bar{n}-1} m_i \right)^{-1} \geq |\mathfrak{f}|^{l\varepsilon/2} |\mathfrak{f}|^{\bar{n}\varepsilon/4} \geq |\mathfrak{f}|^{(l-\bar{n})\varepsilon/4}.$$

We also have

$$(41) \quad |\mathfrak{f}|^{N-\bar{n}} \geq \prod_{i=\bar{n}}^{N-1} m_i \geq \left(\prod_{i=0}^{N-1} m_i \right) \left(\prod_{i=0}^{\bar{n}-1} m_i \right)^{-1} \geq |\mathfrak{f}|^{N\varepsilon/2} |\mathfrak{f}|^{\bar{n}\varepsilon/4}.$$

Therefore $M := N - \bar{n} \geq N\varepsilon/2 + \bar{n}\varepsilon/4 = N\varepsilon/2 - (N - M)\varepsilon/4 \geq N\varepsilon/4$. So there is a subset $B \subseteq \mathcal{O}$ such that

- (1) $\mathfrak{p}^{N'} B \subseteq A$ for $N' \leq N(1 - \varepsilon/4)$,
- (2) $\pi_{\mathfrak{p}^M}(B)$ is a regular set for $M \geq N\varepsilon/4$,
- (3) $|\pi_{\mathfrak{p}^i}(B)| \geq |\mathfrak{f}|^{i\varepsilon/4}$ for any $1 \leq i \leq M$.

Hence by Lemma 31 for $C_1 \gg_{\varepsilon, e} 1$ and $e_0 \leq e$ we have $\text{gr}_{e_0 i}(\langle B \rangle_{C_1}) \neq 0$ for any $0 \leq e_0 i \leq M - 1$. Since it is enough to prove the theorem for λA for some $\lambda \in \mathcal{O}^\times$, we can assume that $0, 1 \in \langle B \rangle_{2C_1}$. Therefore by Proposition 29, we have

$$\pi_{\mathfrak{p}^{\lfloor 2\delta_0 M \rfloor}}(\mathfrak{p}^{e_0 \lceil \delta_0 M / e_0 \rceil} \mathbb{Z}x) \subseteq \pi_{\mathfrak{p}^{\lceil 2\delta_0 M \rceil}}(\langle B \rangle_C),$$

for some $x \in \mathcal{O}^\times$, $\delta_0 := \delta_0(\varepsilon)$, and $C := C(\varepsilon)$. Let

$$N_1 := N' C + e_0 \lceil \delta_0 M / e_0 \rceil, \quad N_2 := N' C + \lfloor 2\delta_0 M \rfloor.$$

Therefore we have

$$\pi_{\mathfrak{p}^{N_2}}(\mathfrak{p}^{N_1} \mathbb{Z}x) \subseteq \pi_{\mathfrak{p}^{N_2}}(\langle A \rangle_C),$$

and

$$N_2 - N_1 = \lfloor 2\delta_0 M \rfloor - e_0 \lceil \delta_0 M / e_0 \rceil \geq \delta_0 M - 2 \geq N\varepsilon\delta_0/8,$$

(notice that, for $N \ll_\varepsilon 1$, we can set $N_1 = N_2$) and

$$N_2 \leq NC.$$

□

REFERENCES

- [Bor08] J. Bourgain, *The sum-product in \mathbb{Z}_q with q arbitrary*, J. Analyse Math. **106** (2008) 1–93.
- [BKT04] J. Bourgain, N. Katz, T. Tao, *A sum-product estimate for finite fields and applications*, GAFA **14** (2004) 27–57.
- [BG09] J. Bourgain, A. Gamburd, *Expansion and random walks in $\text{SL}_d(\mathbb{Z}/\mathfrak{p}^n\mathbb{Z})$:II. With an appendix by J. Bourgain*, JEMS **11**, no. 5., (2009) 1057–1103.
- [LV] E. Lindenstrauss, P. Varjú, work in progress, June 2014.
- [Man42] H. Mann, *A Proof of the fundamental theorem on the density of sums of set of positive integers*, Ann. of Math., 2nd Series, **43** no. 3, (1942) 523–527.
- [SG-a] A. Salehi Golsefidy, *Super approximation, I: \mathfrak{p} -adic semisimple case.*, preprint.
- [SG-b] A. Salehi Golsefidy, *Super approximation, II: the \mathfrak{p} -adic and bounded power of square-free integers cases.*, preprint.

MATHEMATICS DEPT, UNIVERSITY OF CALIFORNIA, SAN DIEGO, CA 92093-0112

E-mail address: golsefidy@ucsd.edu